Probability of Loss of Crew Achievability Studies for NASA's Exploration Systems Development

Roger L. Boyer[a], Mark Bigler[a], and James H. Rogers[b]
[a] NASA Johnson Space Center, Houston, TX USA
[b] NASA Marshall Space Flight Center, Huntsville, AL USA

Abstract: Over the last few years, NASA has been evaluating various vehicle designs for multiple proposed design reference missions (DRM) beyond low Earth orbit in support of its Exploration Systems Development (ESD) programs. This paper addresses several of the proposed missions and the analysis techniques used to assess the key risk metric, probability of loss of crew (LOC). Probability of LOC is a metric used to assess the safety risk as well as a design requirement. These risk assessments typically cover the concept phase of a DRM, i.e. when little more than a general idea of the mission is known and are used to help establish "best estimates" for proposed program and agency level risk requirements. These assessments or studies were categorized as LOC achievability studies to help inform NASA management as to what "ball park" estimates of probability of LOC could be achieved for each DRM and were eventually used to establish the corresponding LOC requirements. Given that details of the vehicles and mission are not well known at this time, the ground rules, assumptions, and consistency across the programs become the important basis of the assessments as well as for the decision makers to understand.

Keywords: PRA, Human Space Missions, Probability of Loss of Crew.

1. INTRODUCTION

Prior to the termination of the Space Shuttle program, the U.S. National Aeronautics and Space Administration (NASA) had been developing a capability to continue supporting the International Space Station (ISS) in Low Earth Orbit (LEO) as well as going beyond LEO. This paper is focused on the work of going beyond LEO for human exploration of space. NASA's Exploration Systems Development (ESD) division has divided this effort into three programs: the Multi-Purpose Crewed Vehicle (known as Orion) program to build the spacecraft, the Space Launch System (SLS) program to build the launch vehicle, and the Ground Systems Development and Operations (GSDO) program to build the ground processing and launch pad facilities. NASA has been evaluating various vehicle designs for multiple proposed design reference missions (DRM) beyond LEO. This paper addresses several of the proposed missions and the analysis techniques used to assess the key risk metric, probability of loss of crew (PLOC). PLOC is a metric used to assess the safety risk as well as being a design requirement. The focus here is to describe the risk assessments that NASA uses during the concept phase of a DRM, i.e. when little more than a general idea of the mission and the vehicle design are known, to establish a "ball park" estimate of PLOC that can be used to set PLOC requirements for the programs.

NASA has entered a new era in space exploration where it will build the capabilities to send humans deeper into space than ever before. One of the first steps is to identify and develop the basic elements for going beyond Earth orbit. This requires some re-inventing from the past and some out-of-the-box, innovative thinking to go beyond the moon. Human space travel beyond LEO is still a pioneering effort. With budgets and schedules to contend and embrace, crew safety is still a primary objective and a challenge. The current plan is to utilize a spacecraft similar to the Apollo capsule with upgrades,

a hybrid launch vehicle utilizing both Saturn V and Space Shuttle features, and a launch pad designed to accommodate both in a launch configuration with current technology. The initial program name for integrating the Orion, SLS, and GSDO programs is currently referred to as the Cross Program. Given these basic elements, a spectrum of possible mission objectives can be achieved. A simple mission would be to orbit the moon or travel to one of the Earth-Moon Lagrange points. A more complex mission would be to go to an asteroid that has been robotically retrieved (or redirected) from some remote location and moved to some high orbit around the moon, where the Orion spacecraft can rendezvous with it so the crew can perform one or more Extravehicular Activities (EVAs) to collect samples. More advanced DRMs, such as to Mars, will require multiple launches of various forms of SLS (i.e. different lift capabilities), additional elements that will come later (e.g. a lander, habitat module, and a propulsion module), as well as requiring much longer mission durations.

2. PRA IN HUMAN SPACE PROGRAMS TODAY

As with any human space program to date, there is a massive effort to integrate each individual program into one program to perform a specified mission. PRA is one of the tools for integrating these programs in order to assess the PLOC and serve as the primary means of verifying the programs' PLOC requirements instead of flying many uncrewed missions upfront to demonstrate it.[1] With PRA present and used from the beginning of the Cross Program, the following three questions were asked and answered to identify the risk drivers:

1. What can go wrong?
2. How likely is it to occur and what is its corresponding uncertainty?
3. What is the consequence of these events?

Identifying these risk drivers early in the program has resulted in many of them being addressed by design changes with minimal cost for the ascent and Entry, Descent, and Landing (EDL) phases. The "in-space" phase has yet to be defined by the selection of the first DRM to fly. Analysing the various DRMs on the table to date have helped in identifying potential in-space risk drivers for the designers to address.

3.0 ACHIEVABILITY STUDIES

NASA began looking for a more intuitive approach in establishing its new LOC requirements for future human space programs instead of just setting an unattainable goal. Achievability studies represent a step in that direction.[2] An achievability study is technically not a PRA, because it is not a scenario based approach.[3] It can use results from previous PRAs that are relevant to the current situation, which can then be combined with new information to make an assessment of the potential risk for future programs. For example, human spacecraft in LEO (e.g. the Space Shuttle and the previous Orion design, which both had comprehensive PRAs) have similar systems as spacecraft headed to the moon, thus adjustments can be made for the differences in mission duration, micro-meteoroid and orbit debris (MMOD) exposure, number of engine firings, etc.

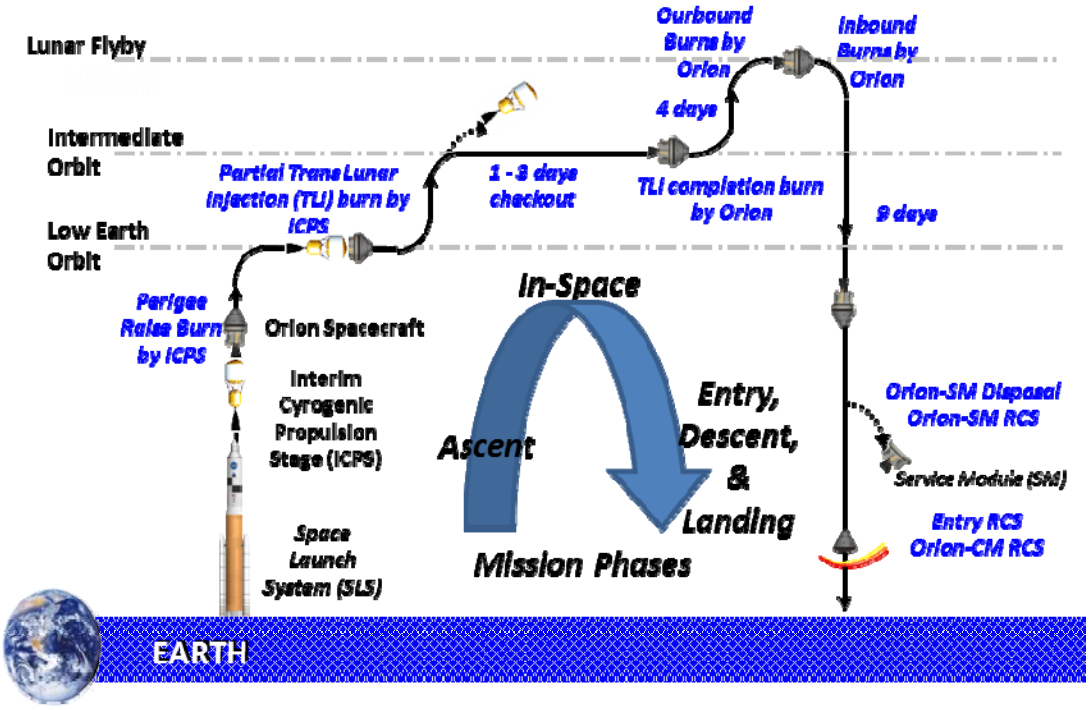
These achievability studies, or risk assessments, are used to help establish "best estimates" for proposed program and agency level design capability risk requirements. The term "design capability" was established to guide the data analysts in understanding the "target" failure rates and probabilities as constant and after initial problems or bugs have been worked out, as well as for communicating with management and engineering. These assessments or studies were categorized as PLOC achievability studies to help inform NASA management as to what "ball park" estimates of probability of LOC could be achieved for each DRM and were eventually used to establish the corresponding PLOC requirements. Given that details of the vehicles and mission are not well known at this time, the ground rules, assumptions, and consistency across the programs become the important basis of the assessments as well as for the decision makers to understand. For a program (especially a human space program) at its conceptual design phase, unknown-unknown risks are real and can be a dominant contributor in actual risk. However, it is difficult to estimate and design against these risks since they

are unknown, unknowns. For example, some material property that degrades to a point of failure in a space environment at some point between here and Mars that has not been detected or observed to date would be an unknown, unknown. These are not addressed in an achievability study, but are better identified through a rigorous testing program.

4.0 POTENTIAL DESIGN REFERENCE MISSIONS

Some of the DRMs being evaluated include a variety of missions to the moon and back as part of the checkout of the new Orion spacecraft with crew on-board. Figure 1 provides an overview of one of the DRMs being evaluated, the Hybrid DRM. The Hybrid DRM begins with the launch of the SLS, the Interim Cyrogenic Propulsion Stage (ICPS), and the Orion spacecraft together as an integrated vehicle. During ascent, Orion's launch abort system can be used to pull the crew to safety if sufficient warning time is available for something that may go wrong. Following the separations of the solid rocket boosters (SRBs) and the core stage with its four rocket engines similar to the Space Shuttle Main Engines (SSMEs), the ICPS and Orion continue to orbit where the ICPS engine fires to circularize the orbit. The ICPS again fires to put Orion in a partial trans lunar injection (TLI) path. A second phase of abort scenarios exist post-circularization when an early return to Earth may be possible. Otherwise, it may become a race with the clock as observed with Apollo 13. For the next one to three days, the crew can check out the Orion spacecraft systems before committing to the remainder of the TLI burn using Orion's service module (SM) engines. Again, if an early return is warranted, options are available to the crew depending on their location in the TLI path. Using the gravity of the moon to pull Orion and throw it back to Earth, Orion will travel back in about nine days. Upon reaching Earth, the SM will separate from Orion before entering the Earth's atmosphere. After re-entry, the parachutes are deployed, the capsule lands in the Pacific Ocean off of California's coast, and a recovery vessel collects the capsule prior to the crew exiting. Problems can occur at any point along the way and the solution will vary based on its location in the mission.

Figure 1: Hybrid Crewed Lunar Flyby DRM Chart



For the PLOC achievability studies performed to date, little was really known about the vehicle design and its mission. Therefore, simplifying assumptions were made in order to perform these assessments. The purpose of the PLOC achievability studies is to help understand the risk associated with the

vehicle and its mission. This information can be used to establish the corresponding mission PLOC requirements, which are used to establish the vehicle design and operations as well as to optimize the DRM with respect to safety.

Although these assessments are at a high level due to the relatively pre-mature nature of the design process, it is assumed that the design is mature or of a design capability nature. This means that the failure probabilities are based on the flat part of the bath tub curve where many of the initial integration related failures have been uncovered and resolved.

This does not mean that first (or early) flight risk is neglected, but that it is analysed separately and communicated to management and the crew. When looking at flight history, one notices that it is not uncommon for one or more failures to occur during the first five launches. A majority of these failures are not hardware related. They are integration failures, software failures, and human errors. For example, stage separation of the launch vehicle is a very critical and risky event, as well as any close proximity events of separation and docking. It is also very easy to get complacent due to previous successes.

Other DRMs include high lunar orbit (HLO), direct retrograde orbit (DRO), and asteroid redirect crewed mission (ARCM). HLO is a mission to orbit the moon for several days, then return. DRO is also a lunar orbit but at a much larger orbit where it takes about six days to partially orbit the moon. This orbit is consistent to where an asteroid would be parked after a robotic mission retrieves it from its current location to one in orbit around the moon for a future crewed mission would rendezvous with it. ARCM is the actual crewed mission of rendezvousing with the asteroid, collecting samples, and returning to Earth. Each of these DRMs represents a progression of mission risk from the Hybrid DRM described above. These DRMs are summarized and compared in Table 1 below for several of the key mission attributes. For example, the Hybrid DRM represents a relatively short mission with more time in Earth vicinity to return home if problems occur early in the mission, while the HLO DRM represents the same amount of time as the Hybrid but with a larger crew and more time away from Earth. The DRO DRM is a much different type of lunar orbit requiring about twice as much time away and the ARCM DRM follows the same path as DRO but with rendezvous, docking, and EVA at an asteroid. Each DRM represents additional risk contributors to be assessed.

Note that the risk estimates increase for the ARCM DRM with the need to rendezvous and dock with the asteroid transfer vehicle and the crew performing EVAs in close proximity of an asteroid with an unknown environment (e.g. dust and sharp edges). Dust can lead to undesired events with space suit joints and may be carried back into the spacecraft to do additional damage. Sharp edges can puncture or tear space suits. Both spacecraft systems and the crew are very careful when docking with objects as damage can result from collisions that may affect the spacecraft structure, heat shield, parachutes, etc.

Table 1: Comparison of Key Design Reference Mission Attributes

DRM Information	HLO DRM	DRO DRM	Hybrid DRM	ARCM DRM
Mission Duration	14 Days	25 Days	14 Days	25 Days
Crew Size	4	2	2	2
ICPS MMOD Exposure in LEO	5 Hours	5 Hours	~3 Hours	5 Hours
Time Spent in Earth's Vicinity	5 Hours	5 Hours	~30 Hours	5 Hours
# of Major SM Prop Burns	3	7	3	7
Return Type	Propulsive	Propulsive	Free Return	Propulsive
Contingency EDL During 1st 30 Hours of DRM	On the Order of Days	On the Order of Days	On the Order of Hours	On the Order of Days
Docking/Undocking	N/A	N/A	N/A	1
EVA	N/A	N/A	N/A	Two, 2-crew, 4 hours each

5.0 ACHIEVABILITY STUDY TECHNIQUES

Achievability studies to date for lunar vicinity missions typically divide up the mission into three phases as shown in Figure 1: 1) pre-launch and ascent, 2) in-space, and 3) entry, descent, and landing (EDL). The Cross Program currently has PLOC requirements for the Orion and SLS programs divided into their relevant association with the ascent and EDL phases of the overall mission.

Based on the almost dozen DRMs (including Mars and near Earth asteroid missions) and the thousands of system level assessments assessed to date, mission duration is the biggest driver for risk to the early crewed missions (14 to 25 days). Mission duration drives the operation time of the hardware, the exposure to MMOD, and the crew health risk. The next major risk driver will be the number of launches required for a given DRM, primarily from a probability of loss of mission viewpoint. With only one launch required for the early crewed missions, mission duration is the dominant driver. Missions to Mars will require multiple launches of the hardware and crew to orbit and/or to Mars.

Software risk is expected to increase for our future human space missions as more automation is used and less crew actions are needed. Therefore, human error for these relatively short and simple missions will likely be less of a contributor than seen in Space Shuttle era assessments that used little automation while software risk will likely become a greater contributor. In addition, work is being performed to evaluate the effects of long duration (greater than 400 days) space missions on the crew, such as fatigue and low gravity physiological effects. Therefore, the "rule of thumb" for these initial

short duration missions is to assume that software and crew error combined is about the same as what was seen in the Space Shuttle era assessments.

6.0 CONCLUSION

The Cross Program currently has PLOC requirements for the Orion and SLS programs divided into their relevant association with the ascent and descent phases of the overall mission. At this time, HQ is finalizing plans to select the first crewed mission in 2021 as well as establish PLOC thresholds and goals. The mission is expected to be of some form of returning humans to the vicinity of the moon and safely returning them. Variations of this mission are being assessed against mission objectives, current design capabilities, and crew safety. The missions listed in Table 1 are prime candidates. PLOC thresholds are being established to raise a flag when risk is estimated to be larger than the agency is willing to accept, thus requiring the program that violates the threshold to explain why it should be allowed to continue. The PLOC goals are set as a stretch above the programs' PLOC requirements.

Currently, both the ascent and EDL mission phases have been defined by the vehicle selected. The launch vehicle configuration is set and Orion's EDL operation is set, thus engineering is working to improve or optimize the design accordingly. Again, PRA is used as the verification approach to determine whether each PLOC requirement is being met or how plans are being devised to address the major risk drivers.

Hindsight would lead to assessing multiple DRMs as part of a coordinated design process for a true multi-purpose crewed vehicle instead of assuming a single mission is sufficient. However, reality still points to funding and schedule constraints yielding a "quasi" multi-purpose vehicle instead of an unlimited one. By evaluating the various DRMs to date, NASA has had more insight into mission and vehicle design instead of having just evaluated one mission.

References

[1] Technical Probabilistic Risk Assessment (PRA) Procedures for Safety and Mission Success for NASA Programs and Projects, NPR 8705.5A. NASA, June 2010.

[2] Cross Program Probabilistic Risk Assessment Methodology, ESD-10011, Exploration System Development Division, Baseline, NASA, November 2012.

[3] Stamatelatos, M. G., et al. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners, NASA/SP-2011-3421, 2nd Edition. NASA, December 2011.